COLLEGE BESCHERMING PERSOONSGEGEVENS

POSTADRES Postbus 93374, 2509 AJ Den Haag BEZOEKADRES Prins Clauslaan 60
TEL 070 - 88 88 500 FAX 070 - 88 88 501 INTERNET www cbpweb nl

AAN de Minister van Economische Zaken
de heer H.G.J. Kamp
Postbus 20401
2500 EK DEN HAAG

DATUM 1 december 2015
ONS KENMERK z2015-00746
CONTACTPERSOON

UW BRIEF VAN 22 september 2015
UW KENMERK DGBI-R&I / 15127595

ONDERWERP Wetgevingsadvies Uitvoeringswet
EU-Verordening elektronische identiteiten en

Geachte heer Kamp,

Bij brief van 22 september 2015 heeft u het College bescherming persoonsgegevens (hierna: het CBP) gevraagd op grond van het bepaalde in artikel 51, tweede lid van de Wet bescherming persoonsgegevens (hierna: Wbp) te adviseren over de Uitvoeringswet EU-Verordening elektronische identiteiten en vertrouwensdiensten (hierna: de Uitvoeringswet).

Het wetsvoorstel is ter consultatie open gesteld via internet van 8 juli tot en met 8 augustus 2015. In het voorstel dat aan het CBP is voorgelegd zijn de consultatiereacties en de reacties van de Minister van Economische Zaken (hierna: Minister van EZ) daarop verwerkt.

1. Achtergrond van de Uitvoeringswet en rol van het CBP

Vanaf 1 juli 2016 zal de EU-Verordening elektronische identiteiten en vertrouwensdiensten (hierna: de Verordening) rechtstreeks van toepassing zijn in Nederland[1]. Doel van de Verordening is om het vertrouwen in elektronische transacties te vergroten door te voorzien in een gemeenschappelijke grondslag voor veilige elektronische interactie tussen burgers, bedrijven en overheden en bijgevolg ook de doeltreffendheid van publieke en private onlinediensten en elektronische handel in de interne markt van de Europesen Unie te verhogen. De Verordening regelt daartoe het grensoverschrijdend gebruik van elektronische identificatiemiddelen en vertrouwensdiensten tussen de lidstaten van de Europese Unie. De Verordening is vanaf 1 juli 2016 van toepassing op vertrouwensdiensten, inclusief het toezicht daarop, en vanaf 18 september 2018 op de verplichte erkenning van elektronische identificatiemiddelen uit andere lidstaten.

Kern van de Verordening is tweeërlei. Ten eerste regelt de Verordening dat burgers en bedrijven zich met bij de Europese Commissie aangemelde elektronische identificatiemiddelen (zijnde een middel waarmee een persoon aan een ander duidelijk kan maken wie hij is en dat hij het echt is) ook toegang kunnen verschaffen tot onlinediensten die door openbare instanties uit *andere*

[1] http://eur-lex.europa.eu/legal-content/NL/ALL/?uri=CELEX:32014R0910

lidstaten worden aangeboden en waarvoor het gebruik van een elektronisch identificatiemiddel vereist is. Daartoe kent de Verordening een verplichte erkenning van door openbare instanties aangemelde elektronische identificatiemiddelen met een betrouwbaarheidsniveau substantieel of hoog.

Ten tweede is uitgangspunt in de Verordening dat de verlener van vertrouwensdiensten (gedefinieerd als elektronische handtekeningen, zegels, tijdstempels, diensten voor elektronische bezorging en elektronische certificaten voor authenticatie van websites) gevestigd in de ene lidstaat niet wordt belemmerd in het verlenen van zijn vertrouwensdiensten in een andere lidstaat. Voor vertrouwensdiensten regelt de Verordening onder meer de eisen waaronder deze mogen worden aangeboden op de markt, de inrichting van het toezicht daarop, een meldplicht bij veiligheidsinbreuken, de rechtsgevolgen en de grensoverschrijdende erkenning daarvan.

De Verordening maakt zowel feitelijke uitvoeringswerkzaamheden als aanpassing van nationale regelgeving noodzakelijk. Het deel van de Verordening over elektronische identificatie vereist volgens de Memorie van Toelichting bij de Uitvoeringswet enkel feitelijke uitvoering, waarbij de ontwikkeling van een landelijk knooppunt dat grensoverschrijdende identificatie mogelijk maakt een belangrijke rol speelt. Dit knooppunt dient in september 2018 gereed te zijn. Voor het deel van de Verordening dat gaat over vertrouwensdiensten is, naast feitelijke uitvoering, ook wijziging van regelgeving noodzakelijk. De voorgestelde uitvoeringwet bevat hiertoe wijzigingen van de Telecommunicatiewet en verscheiden andere wetten.

Verder schrijft de Verordening voor dat aanbieders van vertrouwensdiensten verplicht zijn een veiligheidsinbreuk of integriteitsverlies met aanzienlijke gevolgen voor de verleende vertrouwensdienst of voor de persoonsgegevens die daarmee worden beheerd binnen 24 uur na ontdekking te melden aan het toezichthoudend orgaan van de lidstaat waar de verlener is gevestigd. In de Uitvoeringswet is door middel van een wijziging van de Telecommunicatiewet het toezicht op de naleving van die meldplicht door het CBP geregeld.

2. Beoordeling van het wetsvoorstel

2.1 Vooraf / algemeen

De Verordening en de daaruit voorvloeiende bepalingen werken rechtstreeks en worden om die reden door het CBP als een gegeven beschouwd. Hetzelfde geldt voor het door de Europese Commissie vastgestelde Uitvoeringsbesluit interoperabiliteit en knooppunt[2]. De Uitvoeringswet voorziet in een aantal wetswijzigingen en -aanvullingen. Een deel van die bepalingen is vanuit het oogpunt van verwerking van persoonsgegevens niet relevant. Wat betreft een ander deel is bijvoorbeeld sprake van het regelen van de samenloop van de meldplicht uit de Verordening met in diverse wetgeving voorkomende andere meldplichten en de regeling van een aantal algemene aspecten rondom toezicht en handhaving. Voorts is de verdere invulling van een aantal bepalingen in de Uitvoeringswet afhankelijk gesteld van de vraag of de daarin opgenomen

[2] http://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:32015R1501

normen nog op Europees niveau zullen worden ingevuld.

In Bijlage III bij de Uitvoeringswet is een implementatietabel gevoegd waarin per artikel uit de Verordening is aangegeven of rechtstreekse werking volstaat, of en welke omzetting in nationaal recht nodig is en of er van aanwezige beleidsruimte gebruik zal worden gemaakt. De keuze om wel of geen gebruik te maken van beleidsruimte kan in de tabel vervolgens worden toegelicht. Voor zover die beleidsruimte er wel is maar niet is toegelicht waarom er geen gebruik van wordt gemaakt, adviseert het CBP dat alsnog te doen.

Het CBP heeft zich bij haar advisering met betrekking tot de Uitvoeringswet beperkt tot het signaleren van een aantal aspecten rondom de ontwikkeling van het knooppunt die de bescherming van de persoonlijke levenssfeer betreffen, hoewel de Uitvoeringswet niet de wettelijke basis van dat knooppunt omvat. In het hiernavolgende onder paragraaf 2.2 zal het CBP hierop nader ingaan.

2.2 Het Knooppunt en de verdere ontwikkeling daarvan
Het knooppunt wordt in de Memorie van Toelichting bij de Uitvoeringswet omschreven als een technische voorziening die Nederlandse openbare instanties in staat stelt om vast te stellen of het een elektronisch identificatiemiddel betreft dat is gemeld bij de Europese Commissie, over welk betrouwbaarheidsniveau dat middel beschikt en die de authenticatie van een persoon oplevert, zodat de openbare instantie kan bepalen of toegang tot de online dienst wordt verleend.

Het knooppunt is door de Verordening verplicht voorgeschreven en moet voldoen aan de vereisten die in het hiervoor vermelde Uitvoeringsbesluit interoperabiliteit en knooppunt zijn opgenomen. Uitgangspunt is dat het knooppunt versleutelde berichten met persoonsidentificatiegegevens naar openbare instanties routeert en dat de beheerder van het knooppunt de gegevens niet zal mogen decoderen of opslaan. Wel mag het knooppunt loggegevens opslaan om incidenten te kunnen reconstrueren conform de eisen uit het Uitvoeringsbesluit. Om tijdig uitvoering te kunnen geven aan de verplichtingen uit de Verordening rond erkenning van elektronische identificatiemiddelen dient het knooppunt volgens de Memorie van Toelichting bij de Uitvoeringswet uiterlijk medio september 2018 gereed te zijn.

Het opslaan van persoonsgegevens
In de Memorie van Toelichting wordt ervan uitgegaan dat het knooppunt geen persoonsgegevens zal opslaan. Het CBP wijst erop dat het technisch gezien niet mogelijk is persoonsgegevens door te leiden zonder dat deze gegevens op enig moment - kortstondig - worden opgeslagen.
Het CBP adviseert dan ook dit bij de Memorie van Toelichting en bij de verdere ontwikkeling van het knooppunt te betrekken.

Ten aanzien van het knooppunt en de ontwikkeling daarvan is een PIA uitgevoerd[3]. In de PIA is een disclaimer opgenomen waarin uiteen wordt gezet dat de PIA is uitgevoerd op een moment dat een groot deel van de voor een PIA benodigde informatie nog niet beschikbaar was. Het gevolg hiervan is, aldus de tekst in de disclaimer, dat de PIA meer het karakter heeft van een verkennend onderzoek ten behoeve van verdere beleids- en besluitvorming dan van een volwaardige risico-analyse op een min of meer voldragen implementatieplan, hetgeen ook uitdrukkelijk de bedoeling van de opdrachtgever was. Daarnaast zijn in hoofdstuk 2 van de PIA de beperkingen van de reikwijdte beschreven, waaronder een aantal belangrijke out-of-scope kwesties en toekomstige ontwikkelingen. Hoewel het knooppunt feitelijk nog ontwikkeld zal moeten worden en daarbij in ieder geval dient te voldoen aan hetgeen in de Verordening en het Uitvoeringsbesluit aan vereisten is opgenomen, wijst het CBP erop dat juist in de beperkingen waarmee de PIA is uitgevoerd een aantal van de belangrijkste risico's liggen voor de verdere ontwikkeling van het knooppunt. Het CBP onderschrijft de in de PIA opgenomen aanbeveling - en acht dit ook van wezenlijk belang - om bij het verdere verloop van het ontwikkeltraject van het knooppunt aanvullende PIA's te laten uitvoeren. Daarbij adviseert het CBP zich daarbij niet te beperken tot de in de PIA aanbevolen aspecten.

Uit de PIA volgen een aantal belangrijke conclusies en aanbevelingen, zowel ten aanzien van het (kunnen) voldoen aan de vereisten van de Wbp, als de belangrijkste risico's rondom de werking van het knooppunt die op dit moment reeds worden gesignaleerd. Het CBP zal op de belangrijkste aspecten uit de PIA in het hiernavolgende ingaan. Belangrijk uitgangspunt bij uitvoering van de PIA is dat het knooppunt zal worden aangesloten op Idensys en dat het knooppunt in eerste instantie alleen wordt opengesteld voor publieke dienstaanbieders.

De verantwoordelijke in de zin van de Wbp

Eén conclusie uit de PIA is dat de rol van verantwoordelijke in de zin van artikel 1, aanhef en onder d, van de Wbp voor de verwerking via het knooppunt niet is ingevuld. In het ontwerp van de Uitvoeringswet die aan het CBP is voorgelegd en waarin de uitkomsten van de PIA zijn verwerkt, is de Minister van EZ als verantwoordelijke aangewezen voor de verwerking van persoonsgegevens die door het knooppunt plaatsvindt. Daarmee is deze onduidelijkheid weggenomen. In de Memorie van Toelichting is verder aangegeven dat de verwerking van gegevens in het kader van het knooppunt noodzakelijk is ter uitvoering van de verplichtingen omtrent erkenning van elektronische identificatiemiddelen in de Verordening en dat dit een goede vervulling van de publieke taak dient zoals bedoeld in artikel 8, e van de Wbp. Daarnaast is de Minister van EZ ook verantwoordelijk voor de ontwikkeling en het beheer van het knooppunt.

In de Memorie van Toelichting is de mogelijkheid beschreven dat de Minister van EZ het feitelijk beheer van het knooppunt uitbesteedt aan een derde, bijvoorbeeld een partij uit Idensys, via een bewerkersovereenkomst. Hoewel bewerkersovereenkomsten niet uitgesloten zijn, wil het CBP in dit verband graag het volgende benadrukken. Zowel de ontwikkeling van Idensys als nationaal

[3] Aan het CBP is versie 1.0 'Privacy Impact Assessment eIDAS-koppelpunt' van 31 juli 2015 voorgelegd.

stelsel voor elektronische identificatie en authenticatie, als de ontwikkeling van het knooppunt dat een grensoverschrijdende rol heeft, zijn zodanig complex, omvangrijk en waarschijnlijk onderling verbonden, dat het risico moet worden voorkomen dat het grondrecht inzake de bescherming van de persoonlijke levenssfeer onvoldoende worden geborgd.

Beveiligingsmaatregelen en datalekken
Op dit moment stellen de lidstaten zeer uiteenlopende eisen aan de beveiliging van verwerkingen van persoonsgegevens. Gelet op het Europese en verbindende karakter van het netwerk aan knooppunten, onderschrijft het CBP de aanbeveling uit de PIA dat de beveiligingseisen voor de knooppunten op Europees niveau moeten worden uitgewerkt en bindend moeten worden opgelegd aan de lidstaten. Daarbij wijst het CBP erop dat indien het knooppunt wordt aangesloten op Idensys en er sprake is van het uitbesteden van diensten van het knooppunt aan andere partijen via bewerkersovereenkomsten, die beveiligingsvereisten, onder verantwoordelijkheid van de Minister van EZ, voldoende waarborgen moeten bieden ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerkingen en dat primair de Minister van EZ dient toe te zien de naleving van die maatregelen.

BSN als bijzonder persoonsgegeven
Het CBP onderschrijft de aanbeveling uit de PIA dat bij omzetting van het BSN in een van het BSN afgeleid uniek identiteitsnummer bij het verstrekken van authenticatiegegevens naar andere lidstaten een expliciete wettelijke basis (een afweging door de formele wetgever) is vereist.
Ook een dergelijk nummer mag ingevolge artikel 24 van de Wbp enkel worden gebruikt voor een specifiek bij die wet omschreven doeleinde.

Belangrijkste risico's
In de PIA worden de belangrijkste risico's voor de burger rondom het gebruik van het knooppunt op dit moment omschreven. Daarbij gaat het om de gevolgen van identiteitsdiefstal, de gevolgen van het doorgeven van onjuiste gegevens en de gevolgen van storingen bij het knooppunt waardoor termijnen voor het indien van een aanvraag niet gehaald kunnen worden.
In de Memorie van Toelichting wordt hierop ingegaan en wordt erop gewezen dat het knooppunt adequaat beveiligd zal worden conform de geldende beveiligingsstandaarden en dat in geval van een incident per geval moet worden bezien welke maatregelen nodig zijn.

Het CBP wijst erop dat bij de ontwikkeling van het knooppunt binnen het stelsel zoals de Verordening dat mogelijk maakt (samengevat: het EIDAS-stselsel) vergelijkbare zorgpunten aan de orde zijn als het CBP bij de ontwikkeling van Idensys heeft gesignaleerd. Het CBP wijst in dat verband op de specifieke zorgpunten uit haar brief van 7 mei 2015[4]. Een van die zorgpunten was dat er sprake is van verschillende partijen met verschillende verantwoordelijkheden die elk een beperkt zicht op hebben op het stelsel, hetgeen onder andere gevolgen heeft voor de vraag wie

[4] https://www.cbpweb.nl/nl/nieuws/cbp-maakt-eerste-analyse-van-eid-stelsel

een burger kan aanspreken, voor beveiliging en voor het toezicht op het stelsel.

3. Conclusie
Het CBP acht een zorgvuldige uitwerking van de uit de Verordening voortvloeiende verplichtingen, zoals de ontwikkeling van het hiervoor besproken knooppunt, van groot belang en adviseert om bij de verdere ontwikkeling daarvan aanvullende PIA's te laten uitvoeren . Wat betreft de Uitvoeringswet adviseert het CBP de Minister in de Memorie van Toelichting te motiveren waarom wel of geen gebruik wordt gemaakt van de beleidsruimte die de Verordening op bepaalde aspecten toelaat.

Dictum
Het CBP adviseert u aan het vorenstaande op passende wijze aandacht te schenken.
Voor een nadere toelichting op het advies houd ik mij graag beschikbaar.

Hoogachtend,
Het College bescherming persoonsgegevens,
Voor het College,

Mr. W.B.M. Tomesen
Lid van het College